مقالهٔ علمی – مروری
ISSN
P: 2788-4155
E: 2788-6441
OPEN ACCESS <https://ghalibqjournal.com/index.php/ghalibqjournal>
DOI: https://doi.org/10.58342/ghalibqj.V.13.I.1.8
تاریخ دریافت: ۲۳/ ۰۸/ ۱۴۰۲
تاریخ پذیرش نهایی: ۲۱/ ۱۲/ ۱۴۰۲
تاریخ نشر: ۰۱/ ۰۱/ ۱۴۰۳
صص: ۱۵۹ – ۱۸۲

حق حریم خصوصی و چالش‌های فراروی آن در عصر تکنالوژی

نگارنده: عبدالرحمن کریمی[۱]

چکیده

حق حریم خصوصی ازجمله حقوقی‌است، که در قوانین بین‌المللی و قوانین کشورهای مختلف جای‌گاه ویژه‌یی داشته و هم‌واره مورد حمایت قانون‌گذاران عرصهٔ بین‌المللی و داخلی کشورها بوده است. عصر اطلاعات و تکنالوژی دیجیتال باعث تغییرات عمده‌یی در جامعه شده و هم‌چنین با خود تهدیداتی برای حریم خصوصی افراد به هم‌راه دارد. درک چالش‌ها و تهدیدات این عصر برای حریم خصوصی افراد اهمیت بالایی دارد. هدف این تحقیق بررسی چالش‌های حریم خصوصی و موارد نقض آن به‌وسیلهٔ تکنالوژی در عصر دیجیتال است. پرسش تحقیق این بوده است که: چالش‌های حریم خصوصی در عصر تکنالوژی چیست؟ و تکنالوژی در چه مواردی باعث نقض حریم خصوصی افراد شده است؟ در این تحقیق، از روش تحلیلی – توصیفی با استفاده از ابزار کتاب‌خانه‌یی برای جمع‌آوری اطلاعات استفاده شده است. یافته‌های این تحقیق نشان می‌دهند که تکنالوژی در عصر فعلی یکی از بزرگ‌ترین تهدیدها برای حریم خصوصی‌است و در مواردی نظیر نقض داده‌ها، حملات سایبری، باج‌گیری سایبری، مهندسی اجتماعی، دزدی هویت، دست‌رسی به اطلاعات از طریق شبکه‌های وای‌فای ناامن و عمومی، آسیب‌پذیری اطلاعات از طریق اینترنت اشیا، قرارگرفتن اطلاعات در دید عموم، نفوذ به حریم خصوصی از طریق داده‌کاوی و پروفایل‌سازی و جاسوسی سایبری، باعث نقض حریم خصوصی افراد می‌شود.

واژه‌گان کلیدی: تکنالوژی، حریم خصوصی، چالش‌ها، اینترنت.

[۱] کادر علمی دیپارتمنت اداری – دیپلماسی، پوهنځی/ دانش‌کدهٔ حقوق و علوم سیاسی، مؤسسهٔ تحصیلات عالی هریوا، هرات، افغانستان
(karimiabdulrahman205@gmail.com)

Review Article
ISSN
P: 2788-4155
E: 2788-6441
Ghalib
Received: 14/ 11/ 2023
Accepted: 10/ 02/ 2024
Published: 20/ 03/ 2024
OPEN ACCESS <https://ghalibqjournal.com/index.php/ghalibqjournal>
DOI: https://doi.org/10.58342/ghalibqj.V.13.I.1.8 PP: 159 - 182

Privacy Right and its challenges in the age of technology

Author: Abdulrahman karimi*

Abstract

Privacy is a legal right that holds a special place in international laws and the laws of various countries. It has always been protected by lawmakers in the international and domestic arena. The era of information and digital technology has brought about significant changes in society, along with threats to individuals' privacy. Understanding the challenges and threats to privacy in this era is of great importance. The aim of this research is to examine the challenges to privacy and instances of its violation through technology in the digital age. The research question is what are the challenges to privacy in the age of technology, and in what cases has technology led to the violation of individuals' privacy? This research utilizes an analytical-descriptive method and employs library tools for data collection. The findings of this research show that technology is one of the biggest threats to privacy in the current era. Instances such as data breaches, phishing attacks, cyber extortion, social engineering, identity theft, unauthorized access to information through insecure public Wi-Fi networks, information vulnerability through the Internet of Things, exposure of information to the public, invasion of privacy through data mining and profiling, and cyber espionage all contribute to the violation of individuals' privacy.

Keywords: Technology, Privacy, Challenges, Human Rights.

GHALIB (Research and Scientific quarterly Journal of Ghalib University)
13th years and Volume, First Issue, 2024

* Administrative –Diplomacy Department, Faculty of Law and Political Sciences, Hariva Higher Education Institution, Herat, Afghanistan (karimiabdulrahman205@gmail.com)

۱. مقدمه

در دنیای به‌هم‌پیوستهٔ فن‌آوری اطلاعات و ارتباطات، تحولات سریع درحال رُخ‌دادن است و فرصت‌ها و سهولت‌های بی‌سابقه‌یی را به ارمغان آورده است. این پیش‌رفت‌های تکنالوژیکی نحوهٔ برقراری ارتباط، اشتراک‌گذاری اطلاعات و روش زنده‌گی روزمرهٔ ما را به‌طور اساسی تغییر داده است. با این‌همه مزایا، چالش‌های اساسی نیز وجود دارد و بیش‌ترین توجه به حفظ حریم خصوصی و امنیت دیجیتال معطوف شده است. حفظ حریم خصوصی و امنیت دیجیتال به‌عنوان یکی از دغدغه‌های اصلی در عصر فن‌آوری اطلاعات و ارتباطات محسوب می‌شود.

همان‌طور که در حوزهٔ دیجیتال فعالیت می‌کنیم، ردّ پای دیجیتال ما در تمامی جوانب زنده‌گی مان، از اهداف شخصی و حرفه‌یی تا تفریحات گسترش می‌یابد و ما را در معرض جذابیّت‌ها و خطرات این دنیای فن‌آوری‌محور قرار می‌دهد. زنده‌گی دیجیتال ما، با شبکه‌های پیچیدهٔ پروفایل‌های رسانه‌های اجتماعی، معاملات مالی آنلاین، ذخیره‌سازی داده‌های مبتنی بر ابر و سایر عوامل، به‌طور فزاینده‌یی در معرض تهدیداتی قرار می‌گیرد که می‌تواند اطلاعات شخصی، رفاه مالی و حتا امنیت ما را به خطر اندازد.

اهمیت این موضوع از آن‌جهت است که در عصر فن‌آوری اطلاعات و ارتباطات (ICT)[۲] که زنده‌گی روزمرهٔ ما به‌طور جدانشدنی با دست‌گاه‌های دیجیتال و پلتفرم‌های آنلاین درهم‌تنیده شده است؛ مفهوم حریم خصوصی دیجیتال به‌طور فزاینده‌یی حیاتی شده است. حریم خصوصی دیجیتال به محافظت از اطلاعات شخصی، فعالیت‌های آنلاین و ارتباطات ما در برابر نفوذ، نظارت و سوءاستفادهٔ غیرقانونی مربوط می‌شود. این فقط یک موضوع راحتی یا ترجیح شخصی نیست. این یک حق اساسی و حفاظتی در برابر طیف وسیعی از خطرات احتمالی است، که هم‌واره باید مورد توجه سازمان‌ها و شبکه‌های مختلف و کارگذاران آنلاین قرارگرفته و حمایت قانونی و حقوقی دولت‌ها را به هم‌راه داشته باشد. در عصری‌که داده‌ها اغلب به‌عنوان ارز جدید تبلیغ می‌شوند، حفاظت از حریم خصوصی دیجیتال یک گام پیش‌گیرانه در حفظ امنیت شخصی، حفاظت از شهرت آنلاین و اطمینان از این‌که می‌توان از مزایای (ICT) بدون خطرات غیرقابل استفاده بهره برد، می‌باشد؛ بنابراین، درک این تهدیدها برای افراد و سازمان‌ها برای محافظت مؤثر از حریم خصوصی در عصر تکنالوژی بسیار مهم و حیاتی تلقی می‌شود.

تحت عنوان حریم خصوصی و چالش‌های فراروی آن در عصر تکنالوژی، مشخصاً تحقیقی صورت نگرفته است؛ اما وجود تحقیقات در این حوزه و پیرامون این موضوع را نمی‌توان نادیده گرفت. در زیر به برخی از تحقیقاتی که در گذشتهٔ حوزهٔ تحقیق فعلی صورت گرفته است، اشاره

[2] (information and communication technology)

می‌شود: مصطفوی اردبیلی (۱۴۰۲)، در پژوهشی تحت عنوان «تأثیر هوش مصنوعی بر نظام حقوق بشر بین‌الملل»، به بررسی نقش هوش مصنوعی بر نظام حقوق بشر بین‌المللی پرداخته‌اند. عبداله‌زاده و حاجی پورکندرود (۱۴۰۱) در پژوهشی تحت عنوان «تحلیل چالش‌های دولت الکترونیک با حریم خصوصی اطلاعاتی شهروندان»، به بررسی چالش‌های دولت الکترونیک در حریم خصوصی شهروندان پرداخته‌اند. علی حسینی و دیگران (۱۳۹۹)، در پژوهشی تحت عنوان «امنیت محتوای داده‌ها در حریم خصوصی و مطالعۀ تطبیقی آن»، به بررسی امنیت داده‌های حریم خصوصی به‌صورت تطبیقی پرداخته‌اند. فتحی و شاه‌مرادی (۱۳۹۶)، در پژوهشی تحت عنوان «گسترۀ قلم‌رو حریم خصوصی در فضای مجازی»، به بررسی محدودۀ قلم‌رو حریم خصوصی در فضای مجازی پرداخته‌اند. جنبۀ نوآوری تحقیق حاضر این است که در این تحقیق چالش‌های حریم خصوصی در ابعاد مختلف در عصر تکنالوژی و فن‌آوری اطلاعات پرداخته شده است.

هدف این تحقیق بررسی چالش‌های حریم خصوصی و موارد نقض آن به‌وسیلۀ تکنالوژی در عصر دیجیتال است. پرسش تحقیق این است، که چالش‌های حریم خصوصی در عصر تکنالوژی چیست و تکنالوژی در چه مواردی باعث نقض حریم خصوصی افراد شده است؟ در این تحقیق، از روش تحلیلی – توصیفی با استفاده از ابزار کتاب‌خانه‌یی برای جمع‌آوری اطلاعات استفاده شده است. یافته‌های این تحقیق نشان می‌دهند که: تکنالوژی در عصر فعلی یکی از بزرگ‌ترین تهدیدها برای حریم خصوصی است و در مواردی نظیر نقض داده‌ها، حملات سایبری، باج گیری سایبری، مهندسی اجتماعی، دزدی هویت، دست‌رسی به اطلاعات از طریق شبکه‌های وای‌فای ناامن و عمومی، آسیب‌پذیری اطلاعات از طریق اینترنت اشیا، قرارگرفتن اطلاعات در دید عموم، نفوذ به حریم خصوصی از طریق داده‌کاوی و پروفایل‌سازی و جاسوسی سایبری، باعث نقض حریم خصوصی افراد می‌شود.

۲. مفهوم حریم خصوصی

دامنۀ حریم خصوصی را می‌توان براساس فرهنگ ملّی و ویژه‌گی‌های خاص فردی تدوین کرد. اما موضوعات مشترکی وجود دارد که می‌توان برای تعیین مرزهای کلی حوزۀ زنده‌گی خصوصی، مورد بحث قرار داد. به‌طور کلی دامنۀ حریم خصوصی تا حدی با محرمانه‌بودن اطلاعات شخصی و حفاظت از آن‌ها (دست‌رسی، استفاده، انتشار، انتقال و غیره) هم‌پوشانی دارد؛ به‌همین دلیل هر شخص حق دارد از داده‌های شخصی خود محافظت کند (Radi & Iriana, 2020: 5289). برخی از نشانه‌ها برای ادراک حریم خصوصی، تأثیرگذار اند؛ این نشانه‌ها

شامل فرهنگ فردی و رفتارهای افراد دیگر، مکانیسم‌ها و هنجارهای توصیفی – تقلیدی، رفتار متقابل و مشاهدۀ افراد دیگر که اطلاعات را آشکار می‌کنند، می‌شود (Alessandri, laura & George, 2015: 514).

حریم، واژۀ عربی است که از ریشۀ حرم به معنای منع و تشدید اقتباس گردیده و عبارت از چیزی است که لمس آن حرام بوده و نباید به آن نزدیک شد (رئوفی و هم‌کاران، ۱۳۹۹: ۱۳۸). در لغت‌نامۀ معین، حریم آن‌چه پیرامون خانه و عمارت که بدان متعلق باشد و عبارت از مکانی بیان شده‌است که حمایت و دفاع از آن واجب باشد (۱۳۶۳: ۱۳۵۲). حریم در دو صورت مفرد و مرکب به‌کار می‌رود. در مفهوم مفرد حریم به معنای شریک، دوست و هم‌چنین به معنای شئ است، که مس آن حرام است و نباید به آن نزدیک شد. در مفهوم مرکب، حریم برخی اوقات به مال و در برخی اوقات به انسان اضافه می‌شود. در مفهوم دوم، در صورتی‌که به مال اضافه شود، به معنای اطراف و پیرامون است. مثل حریم چاه؛ و در صورتی‌که حریم به انسان اضافه شود، به معنای چیزی است که باید از آن دفاع شود و به خاطر آن جنگید. با این مفهوم حریم به معنای جان، آبرو، اهل‌وعیال و اموال انسان مترادف است (رئوفی و هم‌کاران، ۱۳۹۹: ۱۳۸–۱۳۹ و موسوی بجنوردی، نسترن پور، ۱۳۹۷: ۳).

در مفهوم اصطلاحی از حریم تعاریف متعددی وجود دارد. در یک تعریف، حریم به مواضع و مکان‌های نزدیکی اشاره دارد که استفاده از آن نیازمند به آن مواضع باشد. مانند به‌سوی آب و محل ریختن خاک (علامه حلی، ۱۴۱۴ق: ۴۱۳). در تعریفی دیگر، حریم خصوصی عبارت از چیزی است که حفظ و نگه‌داری آن واجب و هتک حرمت و احترامش، ممنوع است (مازندرانی، ۱۳۸۲: ۲۹).

حریم هر چیزی، مقدار و اندازه‌یی است که بهره‌برداری کامل از آن چیز، وابسته به مقدار است و هیچ فردی نمی‌تواند بدون رضایت صاحب حریم، آن مقدار را احیا کند (خوئی، ۱۴۱۰ق: ۱۵۳). حریم مقداری از اراضی است اطراف ملک و قنات و نهر و امثال آن است، که برای کمال انتفاع از آن، ضرورت دارد. حریم ملک تبعی است، یعنی از توابع ملک است و مالک می‌تواند از حق خود در حریم بلاعوض و یا در مقابل اخذ عوض صرف نظر کند (جعفری لنگرودی، ۱۳۷۸: ۲۱۴ و امامی، ۱۳۸۷: ۱۳۱).

از نظر دکتر ناصر کاتوزیان، مبنای شناسایی حریم، جلوگیری از تضرر صاحب‌ملک، قنات، نهر و چاه است. پس دیگران باید از تصرفی که مضر است، ممنوع شوند و تصرف بدون ضرر مباح است (۱۳۹۴: ۹۸).

کامل‌ترین تعریف از حریم خصوصی را می‌توان به دکتر انصاری منسوب کرد. ایشان در تعریف حریم خصوصی می‌گویند که حریم خصوصی یکی از اساسی‌ترین حقوق بشر است، که ارتباط مستقیم با شخصیت او دارد. این حق عبارت است از حق انسان به تنهابودن، باخودبودن، به‌وسیلۀ دیگران مورد احترام قرارگرفتن، به‌دور از چشم و نگاه کنترول‌کننده‌یی دیگران و رها از تجسس و تفتیش دیگران زیستن. نهایتاً این‌که حریم خصوصی عبارت از فضایی است که نمی‌توان بدون اجازۀ شخص به آن تجاوز یا تعرض کرد و درواقع دست‌رسی به این فضا برای دیگران امکان‌پذیر نیست (۱۳۸۶: ۱۳۹–۲۷۰).

واژۀ حریم در زبان فارسی به‌صورت کلی یکی از سه معانی زیر را افاده می‌کند:

۱. در صورتی‌که مصدر باشد، به‌معنای بازداشتن از چیزی و بی‌بهره‌کردن از چیزی است؛
۲. در صورتی‌که صفت باشد، به‌معنای بازداشت‌شده و حرام‌کرده‌شده، که مس آن جائز نیست؛ چیزی‌که حرام باشد و دست بدان نتوان کرد، چیزی‌که آن را حمایت کنند و جنگ کنند بر آن؛
۳. در صورتی‌که اسم باشد، به‌معنای حرمت و احترام، آبروی مردم، گرداگرد حوض و چاه، پیرامون، دورادور، دوروبر، حوالی و اطراف می‌باشد (اسکندری، ۱۳۸۹: ۱۴۹).

از تعریف فوق به این نتیجه می‌رسیم که حریم خصوصی به مجموعۀ حقوق و آزادی‌هایی اطلاق می‌شود که به افراد اجازه می‌دهد تا از دست‌رسی، استفاده، فاش‌کردن و تغییر اطلاعات شخصی خود در مورد خودشان برخوردار باشند. این حق نقش مهمی در حفاظت از کرامت و آزادی افراد در برابر نفوذ و کنترول دیگران، دولت و نهادهای خصوصی دارد و شامل حریم خصوصی شخصی (اطلاعات شخصی، سلامتی، وضعیت خانواده‌گی)، حریم خصوصی مکانی (منزل و محل کار)، حریم خصوصی ارتباطی (ارتباطات تلفنی و اینترنتی) و حریم خصوصی در قالب داده‌ها و اطلاعات الکترونیکی می‌شود.

کمیسیون بین‌المللی حقوق‌دانان در کنفرانس کشورهای اروپای شمالی در سال ۱۹۶۷ با بیان مصادیق حریم خصوصی دربارۀ حق خلوت بیان می‌دارد، حق خلوت، حقی است که بر اساس آن هرکس به حال خود گذاشته‌شده و با کم‌ترین دخالت دیگران به زنده‌گی خود بپردازد. این حق شامل موارد زیر است:

۱. دخالت در زنده‌گی خصوصی، مسکن و خانوادۀ او؛
۲. هر حمله‌یی به سلامت جسمی و روانی و آزادی اخلاقی یا مصنوعی او؛
۳. هر حمله‌یی به شهرت و اعتبار او؛
۴. هر تفسیر غلطی از کلام و اعمال او؛
۵. افشای ناگهانی امور ناخوش‌آیند مرتبط با زنده‌گی خصوصی‌اش؛

۶. استفاده از نام، هویت و عکس او؛
۷. هر فعالیتی به‌منظور جاسوسی بر روی او، نشستن در انتظار او و مانیتورینگ و محدودکردن فضا برای او؛
۸. توقیف مکاتبات او؛
۹. استفاده با سوءنیّت از ارتباطات کتبی یا شفاهی او؛
۱۰.افشای اطلاعاتی که او به صورت مخالف با قانون حفظ رازهای مربوط به‌شغل و حرفه یک فرد ارائه یا دریافت کرده است (رئوفی و هم‌کاران، ۱۳۹۹: ۱۴۳ – ۱۴۴).

عصر کنونی که با نام عصر دیجیتال مسما شده‌است، حریم خصوصی را تحت عنوان حریم خصوصی در محیط دیجیتال«حریم خصوصی الکترونیکی» تعریف می‌نماید. علاوه بر مستحق‌بودن حمایت قانونی از این حق برای فرد، این حق را می‌توان به‌عنوان حق حفظ دامنۀ اطراف خود ما تعریف کرد که شامل همه چیزهایی هستند که بخشی از ماست. از قبیلِ بدن ما، خانۀ ما، مال، افکار، احساسات، اسرار و هویت. این‌حق به ما این امکان را می‌دهد که انتخاب کنیم که در کدام قسمت‌های این دامنۀ دیگران می‌توانند دست‌رسی پیدا کنند و نحوه و میزان استفاده از آن بخش‌ها را برای افشا و انتخاب کنترول کنیم (Radi & Iriana, 2020, p 5289).

۳. مستندات فقهی و حقوقی حریم خصوصی

حق حریم خصوصی در فقه اسلامی، قوانین و اسناد حقوقی مختلف، ازجمله اسناد بین‌المللی حقوق بشر، قوانین و مقررات کشورها و رویۀ قضایی تضمین شده‌است. این حق براساس اعتبار حقوق انسانی، حقوق شهروندی و حقوق قراردادی شخص مطرح می‌شود. این حق، در شریعت اسلامی مورد تأیید قرارگرفته و از جای‌گاه ویژه‌یی برخوردار است.

در آیۀ ۱۲ سورۀ حجرات، خداوند (ج) می‌فرماید: «يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بعضاً/ ای کسانی‌که ایمان آورده‌اید از بسیاری از گمان‌ها بپرهیزید، که برخی از گمان‌ها گناه است و جاسوسی و پرده‌دری نکنید، و یکی از دیگری غیبت ننمایید» (خرم‌دل، ۱۳۸۸: ۱۰۹۶).

اعلامیۀ حقوق بشر اسلامی در مادۀ ۱۸ با تأکید بر حفظ حریم خصوصی و حمایت از آن چنین صراحت دارد:
الف. هر انسانی حق دارد که نسبت به جان و دین و خانواده و ناموس و مال خویش، در آسوده‌گی زندگی کند؛

ب. هر انسانی حق دارد که در امور زنده‌گی خصوصی خود (در مسکن، خانواده و مال، ارتباطات) استقلال داشته باشد و جاسوسی یا نظارت بر او، با مخدوش‌کردن حیثیت او جایز نیست و باید از او در مقابل هرگونه دخالت زورگویانه در این شئون حمایت شود؛
ج. مسکن در هر حالی حرمت دارد و نباید بدون اجازۀ ساکنین آن یا به‌صورت غیر مشروع وارد آن شد، و نباید آن را خراب یا مصادره کرد یا ساکنینش را آواره نمود.

بنابراین، طبق این مادۀ اعلامیۀ حقوق بشر اسلامی، افراد نباید نظارت شوند، مسکن و ارتباطات شان بررسی شود و اموال شان به‌صورت پنهانی تحت کنترول قرار گیرد و دلیل ممنوعیت این کارها، استقلال فرد در زنده‌گی خصوصی‌اش است که به‌عنوان یک حق برای او در اعلامیه شناخته‌شده است (قهفرخی و مسعودیان، ۱۳۹۱: ۲۱۲).

بر مبنای مادۀ ۱۲ اعلامیۀ جهانی حقوق بشر با حفظ احترام و تأکید بر حمایت قانونی به حریم خصوصی بیان شده است که، زنده‌گی خصوصی یا امور خانواده‌گی یا محل سکونت یا مراسلات کسی نباید در معرض دخالت خودسرانه واقع شود، و نیز به حیثیت و حسن شهرت هیچ‌کس نمی‌توان حمله کرد. هرکس حق دارد در این‌گونه دخالت‌ها یا این‌گونه تجاوزها از پشتی‌بانی قانون برخوردار باشد؛ بنابراین، به‌عنوان یک حق، همه افراد باید در برابر چنین دخالت‌ها و حملاتی که به شخص او وارد می‌شود، به‌صورت قانونی محافظت شوند (انصاری، ۱۳۸۳: ۳۴۴-۳۴۵).

در مادۀ ۱۷ میثاق بین‌المللی حقوق مدنی- سیاسی نیز بر حمایت از حریم خصوصی تأکید شده و چنین تصریح شده‌است: هیچ‌کس نباید در زنده‌گی خصوصی و خانواده و اقامت‌گاه یا مکاتبات مورد مداخلات خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد، هم‌چنین شرافت و حیثیت او نباید مورد تعرض غیرقانونی واقع شود. هرکس حق دارد در مقابل این‌گونه مداخلات یا تعرض‌ها از حمایت قانون برخوردار گردد.

حق حریم خصوصی در اسناد بین‌المللی، برای کودکان نیز مورد توجه بوده است. در مادۀ ۱۶ کنوانسیون حقوق کودک، دخالت و ملاحظات غیرقانونی و خودسرانه و هتک حرمت در امور خصوصی و خانواده‌گی و حتا مکاتبات کودک ممنوع شده و حتا از دولت‌ها خواسته شده‌است که در برابر این‌گونه اعمال، ضمانت اجرایی تعیین کنند. هم‌چنین مادۀ ۱۳ کنوانسیون حقوق کودک با پذیرش حق کودک بر آزادی ابراز عقیده، این حق را شامل آزادی در جست‌وجو، دریافت و رساندن اطلاعات و عقاید از هر نوع می‌داند. مادۀ ۱۴ این کنوانسیون نیز به‌حق آزادی فکر، عقیده و مذهب برای کودکان اشاره دارد (بیستونی و مقدادی، ۱۴۰۱: ۹۷).

در سطح منطقه‌یی، براساس معاهدات مختلف، حق حریم خصوصی نیز مورد تأیید قرار گرفته است. مادۀ ۸ کنوانسیون اروپایی حفاظت از حقوق بشر و آزادی‌های بنیادین سال ۱۹۵۰ می‌گوید: هرکس حق دارد که حریم خصوصی و زنده‌گی خانواده‌گی، خانه و مکاتبات وی مورد احترام قرار داده شود. هیچ مقام دولتی نباید در استفاده از این حق دخالت کند، به‌جز در رعایت قانون و اگر این دخالت برای مصالح امنیت ملّی، امنیت جامعه، رفاه اقتصادی کشور، پیش‌گیری از اختلال یا جرم، حفظ سلامت اخلاقی یا برای حفاظت از حقوق و آزادی‌ها لازم باشد. دیگر اقداماتی که در یک جامعۀ دموکراتیک لازم است.

در نظام حقوقی افغانستان نیز حفاظت از حریم خصوصی مورد توجه قانون‌گذار بوده و در موارد مختلف از رعایت و حفظ حریم خصوصی، سخن گفته شده‌است. به‌طور مثال، مادۀ ۳۷ قانون اساسی «آزادی و محرمیت مراسلات و مخابرات اشخاص چه به‌صورت مکتوب باشد و چه به‌وسیلۀ تلفن، تلگراف و وسایل دیگر، از تعرض مصئون است. دولت حق تفتیش مراسلات و مخابرات اشخاص را ندارد؛ مگر مطابق به‌احکام قانون». مادۀ ۳۸ قانون اساسی «مسکن شخص از تعرض مصئون است. هیچ شخصی، به‌شمول دولت، نمی‌تواند بدون اجازۀ ساکن یا قرار محکمۀ باصلاحیت و به‌غیر از حالات و طرزی که در قانون تصریح شده‌است، به‌مسکن شخص داخل شود یا آن را تفتیش نماید. در مورد جرم مشهود، مأمور مسؤول می‌تواند بدون اجازۀ قبلی محکمه، به مسکن شخص داخل شود یا آن را تفتیش کند. مأمور مذکور مکلف است بعد از داخل‌شدن یا اجرای تفتیش، در خلال مدتی که قانون تعیین می‌کند قرار محکمه را حاصل نماید».

۴. حق حریم خصوصی در عصر دیجیتال

عصر اطلاعات که معمولاً به‌عنوان عصر کمپیوتر یا عصر دیجیتال نیز شناخته می‌شود، دوره‌یی از تاریخ بشر است که با خروج از صنعت سنّتی با اقتصاد مبتنی بر دست‌کاری اطلاعات (جامعۀ اطلاعاتی) از دهۀ ۱۹۷۰ میلادی با معرفی کمپیوتر شخصی با فن‌آوری‌های بعدی آغاز شده‌است. یکی از رایج‌ترین مفاهیم مربوط به نسل چهارم حقوق بشر دست‌رسی به اینترنت و ارتباطات است. وابسته‌گی شدید جوامع انسانی از جنبه‌های گوناگون به یک‌دیگر، گسترش روزافزون جهان مجازی، رُشد بی‌سابقۀ علم و فن‌آوری در عرصه‌های مختلف و ظهور حقوقی مانند حق ارتباطات به منزلۀ یکی از مصادیق نسل چهارم حقوق بشر، باعث شده‌است تا دانش‌مندانی چون برن و ستون فن‌آوری‌های نوین را نسل چهارم حقوق بشر بدانند (مصطفوی اردبیلی و دیگران، ۱۴۰۲: ۹۴).

از آن‌جایی‌که درحال حاضر تکنالوژی پیش‌رفت نموده و امکان نقض حریم خصوصی در فضای سایبر نیز وجود دارد، شورای حقوق بشر به تاریخ ۲۳ مارچ سال ۲۰۱۷، قطع‌نامۀ شماره ۳۴/۷ را در مورد حریم خصوصی در عصر دیجیتال تصویب نمود. بند ده قطع‌نامه از کمیشنر عالی حقوق بشر سازمان ملل درخواست می‌کند تا قبل از نشست سی‌وهفتم شورای حقوق بشر اقدام به سازمان‌دهی کارگاه کارشناسی با هدف شناسایی و تشریح اصول، استانداردها و به‌ترین روش‌های ترویج و حفاظت از حریم خصوصی در عصر دیجیتال کرده و گزارشی از آن را تهیه نموده و در نشست سی‌ونهم شورا ارائه نماید (علی حسینی و هم‌کاران، ۱۳۹۹: ۱۰۸۳).

۵. تکنالوژی و نقض حریم خصوصی

از آن‌جایی‌که جهان به‌طور فزاینده‌یی از طریق فن‌آوری اطلاعات و ارتباطات به هم متصل می‌شود، چشم‌انداز دیجیتال مزایای بی‌شماری را ارائه می‌دهد؛ اما هم‌چنین مجموعه‌یی از تهدیدات را برای حریم خصوصی و امنیت دیجیتال به همراه دارد. درک این تهدیدها برای افراد و سازمان‌ها برای محافظت مؤثر از خود در این عصر فن‌آوری‌محور بسیار مهم است. در این‌جا برخی از رایج‌ترین تهدیدها و چالش موجود حریم خصوصی از طریق ابزارهای تکنالوژی بیان می‌گردد.

۵–۱. نقض داده‌ها

اطلاعات شخصی افراد زیاد است و ممکن است از طریق فعالیت‌های روزانه از قبیل پرداخت وام مسکن، گشت‌وگذار در اینترنت، انجام تراکنش‌های آنلاین و ثبت نام، به‌خطر افتاده و داده‌های شخصی از آن‌جایی‌که به‌راحتی به دست‌رس کارگذاران آنلاین قرار می‌گیرد، نقض شود (Rashidat Taiwo, 2023: 7). نقض داده‌ها زمانی رُخ می‌دهد که مجرمان سایبری به پای‌گاه‌های اطلاعاتی یا سیستم‌های یک سازمان دست‌رسی غیرمجاز پیدا کنند و در نتیجه اطلاعات شخصی و مالی حساس را در معرض دید قرار دهند. نمونه‌های قابل توجه شامل موارد نقض در فیس‌بوک و ایکوفکس[۳] (Equifax) قابل مشاهده است. مشخص است که تکنالوژی امکان سازمان‌دهی گفت‌وگو بین کاربران کمپیوتر شخصی را از طریق اینترنت با استفاده از محیط‌های مختلف تحت عنوان سایت‌های شبکۀ اجتماعی فراهم می‌کند. رسانه‌ها و

[۳] یکی از بزرگترین شرکت‌های ارائه خدمات اطلاعات اعتباری (Credit Reporting) در جهان است. این شرکت در سال ۱۸۹۹ تأسیس شده و مقر اصلی آن در آتلانتا، گرجستان قرار دارد. فعالیت اصلی Equifax در جمع‌آوری، تجزیه و تحلیل و گزارش دادن اطلاعات اعتباری و مالی افراد و شرکت‌هاست.

شبکه‌های اجتماعی، وبلاگ‌ها و میکرو ویب‌لاگ‌ها، ویکی‌ها و بازی‌های چندنفره، عملاً ابـزار مفیدی برای ارتباط بین کاربران و اشتراک‌گذاری اطلاعـات اسـت؛ امـا خطـر احتمـالی بـرای حفاظت از اطلاعات شخصی وجود دارد؛ زیرا ممکن است ایـن اطلاعـات بـه دسـت‌رس افـراد غیرمجاز قرار گیرد (Radi & Iriana, 2020: 5295- 5296). ازسوی دیگر، توهم ایمنی اطلاعات به‌عنوان یک پیش‌فرض، باعث تشویق اشتراک‌گذاری بیش‌تـر اطلاعـات ازسـوی کـاربران در فضای مجازی یا شبکه‌های اجتماعی می‌شود (Alessandri, laura & George, 2015: 510).

۵–۲. حملات سایبری، باج‌افزار و مهندسی اجتماعی

حملات سایبری یا فیشینگ، یک تکنیک فریبنده است که در آن مهاجمان هویت اشخاص یـا افراد قابل اعتماد را جعل می‌کنند تا افراد را فریب دهند و اطلاعات حساسی، مانند اعتبار ورود به سیستم یا جزئیات کارت اعتباری را فاش کننـد. افـزایش حمـلات فیشـینگ، تهدیـد قابـل توجهی برای امنیت و حریم خصوصی کاربران ایمیل است، مهاجمان به‌طور مداوم تکنیک‌های خود را برای سوءاستفاده از قربانیان ناآگاه اصلاح می‌کنند. آخـرین گـزارش ارائـه‌شـده توسـط آژانس امنیت سایبری اتحادیهٔ اروپا (ENISA) در سال ۲۰۲۲ اشاره می‌کند که حملات فیشینگ عموماً مخاطبان گسترده‌یی را هدف قرار می دهند و بنابراین در تعداد زیـادی از اهـداف مـورد استفاده قرار می‌گیرند. این حملات با سایر حملات مهندسی اجتماعی که برای هدف‌قـراردادن کارکنان خاص سفارشی شده‌اند، متفاوت است (Brandqvist, Lieberth Nilsson, 2023: 4).

بدافزارها (نرم افزارهای مخرب) شامل ویروس‌ها، تروجان‌ها و کرم‌هـایی اسـت کـه بـرای به‌خطرانداختن یـا آسـیب‌رسـاندن بـه سیسـتم‌هـای کـامپیوتری طراحـی‌شـده‌انـد. بـاج‌افـزار، زیرمجموعه‌یی از بدافزارها، فایل‌های قربانی را رمزگذاری می‌کنـد و بـرای آزادی آن‌هـا بـاج می‌خواهد. هم‌چنین باید توجه داشت که هکرها با انگیزه‌های مختلف به نقض حریم خصوصی اقدام می‌کنند. در عین‌حال برخی کاربران هم هستند که باانگیزه‌های شخصی، حریم خصوصی کاربران دیگر را نقض می‌کنند. این نقض حریم خصوصی می‌توانـد بـه‌منظـور انتقـام‌جـویی از طریق نشر عکس‌های خصوصی فرد موردنظر صورت گیرد (فتحی و شاه‌مرادی، ۱۳۹۶: ۲۴۰). آژانس امنیت سایبری اتحادیهٔ اروپا اصطلاح باج‌افزار را به‌عنوان «نوعی حمله که در آن عوامل تهدید کنترول دارایی‌های هدف را در دست می‌گیرند و در قبال بازگرداندن در دست‌رس‌بودن و محرمانه‌بودن دارایی، باج می‌خواهند» تعریف می‌کند. طبـق گفتـهٔ اگـری، بـاج‌افـزار یکـی از رایج‌ترین انواع جرایم سایبری در سال‌های اخیر بوده است. همه‌گیری اخیر شاهد افزایش تعداد حملات باج‌افزار بود و از آن زمان تعداد قربانیان باج‌افزار کاهش‌یافته اسـت. رایـج‌تـرین روش

تحویل برای حملات باج‌افزار، فیشینگ از طریق ایمیل است. مؤسسات و شرکت‌های دولتی که در معرض حملات باج‌افزار قرارگرفته‌اند، اغلب تمایلی به بحث دربارۀ چه‌گونه‌گی وقوع آن ندارند؛ اما بسیاری از آن‌ها اذعان دارند که حملات موفقیت‌آمیز نتیجۀ گرفتارشدن کارمندان به ایمیل‌های فیشینگ بوده است (Brandqvist, Lieberth Nilsson, 2023: 4).

حملات مهندسی اجتماعی از روان‌شناسی انسان برای دست‌کاری افراد به‌منظور افشای اطلاعات محرمانه یا انجام اقدامات سوءاستفاده بهره می‌برند، که این عملیات به شدت امنیت را به خطر می‌اندازد. این نوع حملات ممکن است از طریق تماس‌های تلفنی، ایمیل یا تعاملات حضوری رُخ دهد، و در این فرایند، حمله‌کننده سعی می‌کند افراد را ترغیب به ارائۀ اطلاعات حساس کند یا آن‌ها را به انجام اقدامات مشخصی تحریک کند. علاوه‌براین، مهندسی اجتماعی اغلب برای به‌دست‌آوردن جای‌گاهی فنّی در شبکه‌های سازمانی بهره می‌برد. با استفاده از اطلاعاتی که از دست‌رسی به کارمندان در داخل سازمان به‌دست می‌آید، حمله‌کننده‌گان توان‌مندی‌های فنّی خود را تقویت کرده و به اقدامات بیش‌تری در دست‌رس خود دست پیدا می‌کنند. این نشان‌دهندۀ اهمیت حفاظت از اطلاعات داخلی سازمان در برابر حملات مهندسی اجتماعی است و تأکید می‌کند که نه‌تنها تکنالوژی، بل‌که آگاهی و آموزش افراد نیز در افزایش امنیت شبکه‌ها از اهمیت ویژه‌یی برخوردارند (همان‌جا).

۵–۳. دزدی هویّت

سرقت هویت شامل استفادۀ متقلبانه از اطلاعات شخصی یک فرد برای ارتکاب جرایم مختلف، مانند کلاه‌برداری مالی یا جعل هویت آنلاین است. ازسوی دیگر، در بسیاری از موارد ویب‌سایت‌ها نقش «درباز» را بازی می‌کنند؛ کاربران در هنگام ثبت نام اولیه فقط با یک کلیک می‌توانند سیاست حریم خصوصی را بدون خواندن متن بپذیرند. نتیجۀ پذیرش کامل همه شرایط بدون این‌که کاربر واقعاً از آن‌ها آگاه باشد، می‌باشد. در سایر موارد اطلاعات شخصی کاربر، تنها پس از یک‌بار مراجعه ذخیره می‌شود و بدون رضایت مالک به‌صورت خودکار به مرکز منتقل می‌شود. در برخی موارد رسانه‌ها ممکن است اطلاعاتی در مورد سیاست حفظ حریم خصوصی ارائه نکند، یا به اطلاعات شخصی بیش‌ازحد نیاز داشته باشد، که این امر در صورت ثبت نام کاربر باعث نقض حریم خصوصی می‌شود (Radi & Iriana, 2020: 5296).

۵–۴. شبکه‌های وای‌فای ناامن

شبکه‌های وای‌فای عمومی، اگر به‌درستی ایمن نباشند، می‌توانند کاربران را در معرض خطرات مختلفی قرار دهند؛ زیرا هکرها می‌توانند داده‌های ارسال‌شده از طریق این شبکه‌ها را پی‌گیری و نظارت کنند. طبق تحقیقات انجام‌شده توسط لطفی و دیگران؛ استفاده از شبکه‌های وای‌فای ناامن و عمومی اطلاعاتی را از شخص استفاده‌کنندهٔ اینترنت از طریق وای‌فای عمومی، به دست‌رس سازمان‌های اینترنتی قرار می‌دهد. این اطلاعات شاملِ نام کاربر، شمارهٔ تلفن، ایمیل و شناسهٔ کاربر می‌شود (Lotfy &others, 2021: 663-664).

۵–۵. آسیب‌پذیری‌های اینترنت اشیا

این اصطلاح برای توصیف مجموعه‌یی از اشیا و دست‌گاه‌هایی است که به‌منظور ارسال و دریافت داده‌های به‌دست‌آمده با استفاده از حس‌گرها برای نظارت پارامترهای انتخاب‌شده و برای گرفتن تحلیل مقادیر به‌دست‌آمده برای کنترول فرایندها در فضاهای مختلف خانه به اینترنت متصل می‌شوند. دست‌گاه‌های اینترنت اشیا، مانند دوربین‌های هوش‌مند و لوازم‌خانه‌گی، اغلب به‌اندازهٔ کافی امنیت ندارند و می‌توانند توسط مجرمان سایبری برای دست‌رسی به شبکه‌ها و اطلاعات شخصی مورد سوءاستفاده قرار گیرند. اینترنت اشیا از دو جهت می‌تواند حفظ حریم خصوصی را نقض کند. در برخی موارد ممکن است محرمانه‌بودن اطلاعات را مختل کند؛ زیرا هر شئ فیزیکی یا منطقی می‌تواند یک کُد شناسایی منحصربه‌فرد دریافت کند و می‌تواند آزادانه از طریق اینترنت یا از طریق شبکه‌های اجتماعی دیگر ارتباط برقرار کند، که با افزایش تعداد سنسورها منجر به انباشته‌شدن داده‌ها می‌شود و خطرات امنیت و حریم خصوصی را افزایش می‌دهد. از طرف دیگر، امنیت اینترنت اشیا با مجموعه‌یی از کمپیوترها و دست‌گاه‌های اینترنتی مختلف با استفاده از رمزهای عبور سنتی، که محافظت نمی‌شوند، پیکربندی‌شده و ممکن است مورد حملات مختلف قرار گیرند. این حملات اجزایی را با سطح پایین هدف قرار می‌دهند و به دنبال آسیب‌پذیری آن‌ها در برابر هک و دست‌کاری هستند (Radi & Iriana, 2020: 5298).

۵–۶. تهدیدات داخلی

تهدیدات داخلی یا درونی زمانی رُخ می‌دهد که افراد در یک سازمان از دست‌رسی خود برای به خطرانداختن امنیت، چه عمدی یا ناخواسته، سوءاستفاده کنند. با پیش‌رفت تکنالوژی حفاظت از حریم خصوصی به یکی از بزرگ‌ترین مشکلات تبدیل شده‌است؛ و این حوزه از حریم زنده‌گی انسان‌ها معمولاً با توسعهٔ فن‌آوری به چالش کشیده می‌شود (Yu, 2016: 2751).

۵–۷. پی‌گیری و نظارت داده‌ها

پی‌گیری و نظارت و استراق سمع از ترافیک داده می‌تواند اطلاعات حساس را هنگام انتقال از طریق اینترنت در معرض دید قرار دهد؛ به‌خصوص اگر به‌درستی رمزگذاری نشده باشد، خطر سرقت یا فروش داده‌های شخصی، که شامل عکس‌ها، فیلم‌ها و ویدیوهای روی تلفن هم‌راه است و به‌صورت آنلاین ارسال می‌شوند، قابل دست‌رسی برای کارفرمایانی که به‌صورت آنلاین فعالیت دارند. ازسوی دیگر، نظرات در رسانه‌های اجتماعی یا ویب‌لاگ‌ها، ضبط حرکات و رفتارهای افراد توسط دوربین‌های دیجیتال و بی‌احتیاطی‌های جزئی در فضای دیجیتال می‌توانند یک فرد را برای مادام‌العمر تحت‌الشعاع قرار دهند (Rashidat Taiwo, 2023: 11)؛ ازسوی دیگر، با اشتراک‌گذاری اطلاعات از طریق رایانش ابری، تعدادی از کاربران ممکن است به آن دست‌رسی پیدا کنند؛ مثلاً تعداد زیادی از کاربران می‌توانند به داده‌های ذخیره‌شده توسط دست‌گاه‌ها و برنامه‌های مبایل، دست‌رسی داشته باشند که این خود نقض حریم خصوصی داده‌ها تلقی می‌شود (Radi & Iriana, 2020: 5297).

۵–۸. خطرات تشخیص چهره و داده‌های بیومتریک

استفادۀ روزافزون از فن‌آوری تشخیص چهره و داده‌های بیومتریک برای اهداف امنیتی، نگرانی‌هایی را در مورد حریم خصوصی و سوءاستفادۀ احتمالی از این داده‌ها را افزایش می‌دهد. از آن‌جایی‌که این فایل‌ها کمپیوتری هستند، اطلاعاتی‌که در آن‌ها وجود دارد اغلب از طریق شبکه‌هایی در دست‌رس است که بیش از یک سازمان می‌توانند به آن‌ها دست‌رسی داشته باشند. وجود تمام این اطلاعات دیجیتالی در مورد امور خصوصی ما خطراتی را به هم‌راه دارد. اول، افرادی‌که فایل‌ها را نگه‌داری می‌کنند ممکن است از آن‌ها سوءاستفاده کنند. آن‌ها می‌توانند در زنده‌گی شخصی ما فحاشی کنند، تاریخ‌چۀ اعتباری را بدزدند، یا اطلاعات را برای منافع شخصی بفروشند. خطر احتمالی دیگر شامل درز اطلاعات از طریق بی‌احتیاطی یا بی‌کفایتی یا سرقت آن توسط هکرها است؛ حتا در برخی موارد ممکن است این اطلاعات به عمد داده شود (Griffin & others, 2002: 31).

۵–۹. داده‌کاوی و پروفایل‌سازی

سازمان‌ها و پلتفرم‌ها اغلب حجم زیادی از داده‌های کاربر را جمع‌آوری و تجزیه‌وتحلیل می‌کنند، تا پروفایل‌های دقیقی را برای بازاریابی هدف‌مند یا اهداف دیگر ایجاد کنند، که می‌تواند به حریم خصوصی نفوذ کند. پروفایل خودکار گروه‌ها و افراد، یک روش معمول در

جامعهٔ اطلاعاتی است. امکانات روزافزون داده‌کاوی یا جست‌وجوی اطلاعات به‌طور قابل‌توجهی توانایی انجام چنین پروفایلی را افزایش می‌دهد. بسته به کاربرد پروفایل و داده‌کاوی ممکن است خطرات خاصی، مانند تبعیض، فردی‌زدایی و عدم تقارن اطلاعاتی را ایجاد کند. به منظور کاهش ریسک پروفایل های داده کاوی، کارشناسان حوزهٔ علوم کامپیوتری گزینه های سیاستی جای‌گزین و ابزارهای نظارتی را برای مقابله با خطرات داده‌کاوی، پیش‌نهاد می‌کنند (Schermer, 2011: 45).

۵–۱۰. جاسوسی سایبری و حملات دولتی

دولت‌ها می‌توانند از بزرگ‌ترین نقض‌کننده های حریم خصوصی در فضای دیجیتال باشند. پس از حملات یازده سپتامبر، دولت آمریکا و پس‌از آن اکثریت دولت‌ها به این نتیجه رسیدند که در دو راهی حریم خصوصی و امنیت یکی از آن‌ها را باید انتخاب کنند؛ این مسأله منجر به این شد تا طرف امنیت را بگیرند. حاصل این تصمیم برای بعدها شنود تلفن‌های شهروندان آمریکایی و متعاقباً شنود تلفن های سران کشورها بود (فتحی و شاه‌مرادی، ۱۳۹۶: ۲۳۹). دولت‌های ملّی برای سرقت داده‌های حساس، به خطرانداختن زیرساخت‌ها یا مختل‌کردن سیستم های حیاتی به جاسوسی سایبری دست می‌زنند که تهدیدی قابل‌توجه برای امنیت ملّی و حریم خصوصی افراد است. در عصر فن‌آوری، یکی از مسائل مهمی که درحال رُشد است، الکترونیک‌سازی دولت‌ها است که خود می‌تواند باعث نقض حریم خصوصی شهروندان گردد. این ممکن است از چهار طریق باعث خدشه‌دارشدن حریم خصوصی، خاصتاً حریم خصوصی اطلاعات گردد: الف. امکان ثبت کوکی‌ها، گزارش‌ها، آدرس‌های آی پی یا وب‌سایت‌های بازدیدشده توسط شهروندان، به‌راحتی به‌وجود می‌آید و این مسأله ممکن است حریم شخصی را خدشه‌دار سازد؛ ب. چالش داده‌های بزرگ یکی دیگر از مهم‌ترین مسائلی است که باعث خدشه‌دارشدن حریم خصوصی افراد می‌شود. حجم عظیم داده‌ها بر روی وبلاگ‌ها، سایت‌ها، و شبکه‌های اجتماعی به‌طور خودخواسته قرار می‌گیرد، به‌صورت مقادیر ترابایتی درآمده که امکان مطالعهٔ نگرش‌ها، رفتارها و سبک‌های زنده‌گی‌شان را به دولت‌ها که به راحتی به این حجم داده‌ها دست‌رسی دارند می‌دهند؛ هم‌چنین، مطالعهٔ نحوهٔ رُشد و گسترش جریان‌های سیاسی با استفاده از داده‌کاوی چنین داده‌های بزرگی، به راحتی ممکن می‌گردد؛ ج. ادغام داده؛ د. جمع‌آوری مخفیانهٔ داده‌ها (عبداله زاده و حاجی پور کندرود، ۱۴۰۱: ۱۰ و۱۱).

۶. هوش مصنوعی و حریم خصوصی

حق بهره‌مندی از پیش‌رفت‌های علمی ازجمله حقوق اساسی بشر بوده و یکی از این پیش‌رفت‌ها در عرصۀ فن‌آوری، هوش مصنوعی است. هوش مصنوعی نوعی هوش است که در دهۀ ۱۹۵۰ میلادی متولد شد و بخش جدایی‌ناپذیر از انقلاب دیجیتال است. پیش‌رفت هوش مصنوعی و کاربرد آن در بسیاری از حوزه‌های زنده‌گی انسان، به‌ویژه در حوزۀ حقوق انسانی، شیوۀ زنده‌گی انسان‌ها را متحول کرده است (مصطفوی اردبیلی، ۱۴۰۲: ۸۶). دبیر کل سازمان ملل متحد در سال ۲۰۱۹ در کتاب بالاترین آرزو، معتقد است که عصر دیجیتال مرزهای جدیدی را برای رفاه، دانش و اکتشاف انسان گشوده است. وی با تأکید بر این مسأله که تکنالوژی دیجیتال ابزار جدیدی برای دفاع و اعمال حقوق بشر فراهم می‌کند، از نقض حقوق از طریق نظارت، سرکوب، سانسور، آزار و اذیت آنلاین مدافعان حقوق بشر، سخن گفته است. او تأکید کرده است که حکم‌رانی هوش مصنوعی، باید از انصاف، پاسخ‌گویی، توضیح‌پذیری و شفافیت اطمینان حاصل کند. کمیساریای عالی حقوق بشر سازمان ملل متحد در گزارش خویش تأثیرات هوش مصنوعی را در صورت عدم توجه کافی به اثرات آن، منفی و حتا فاجعه‌بار خوانده است (Human Rights Council, 2021: 2).

عمل‌کرد سیستم‌های هوش مصنوعی می‌تواند به تجاوزات به حریم خصوصی و سایر تداخلات به حقوق را با روش‌های مختلف تسهیل و عمیق‌تر کند. این ویژه‌گی هوش مصنوعی است که تداخل با حق حفظ حریم خصوصی را از طریق افزایش جمع‌آوری و استفاده از داده‌های شخصی افزایش داده و تشدید کند. از آن‌جایی‌که سیستم‌های هوش مصنوعی معمولاً بر مجموعۀ دادۀ بزرگ اغلب (داده‌های شخصی) متکی هستند، این انگیزه، جمع‌آوری، ذخیره‌سازی و پردازش گستردۀ داده‌ها را فراهم می‌سازد. بسیاری از کسب‌وکارها خدمات را برای جمع‌آوری داده تا حد امکان بهینه می‌کنند. برای مثال، کسب‌وکارهای آنلاین مانند شرکت‌های رسانه‌یی – اجتماعی بر جمع‌آوری و کسب درآمد از حجم عظیمی از داده‌های مربوط به کاربران اینترنت متکی هستند (Human Rights Council, 2021: 4). وضع قوانین و مقررات نقش مهمی در حفاظت حریم خصوصی دارند. به این‌منظور کشورها می‌توانند سیاست‌های متفاوتی را در حفظ حریم خصوصی سایبری وضع نمایند. در سال ۲۰۱۴ دیوان دادگستری اروپا مقرراتی را وضع کرد، که براساس آن شهروندان اروپایی این حق را دارند که از موتورهای جست‌وجو بخواهند مواردی را که نادرست است یا بیش ازحد تلقی می‌شوند، حذف کنند که به آن حق فراموش‌شدن می‌گویند (Yu, 2016: 2752).

ابزارهای هوش مصنوعی به‌طور گسترده برای جست‌وجوی بینش در مورد الگوهای رفتار انسان استفاده می‌شود. با دست‌رسی به مجموعۀ داده‌های مناسب، می‌توان در مورد این‌که چند نفر در یک محلۀ خاص حضور دارند، چه برنامه‌های تلویزیونی را ترجیح می‌دهند و حتا چه ساعتی تمایل به خوابیدن، بیدارشدن و رفتن دارند، نتیجه‌گیری کرد. ابزارهای هوش مصنوعی می‌توانند استنباط‌های گسترده‌یی در مورد افراد، از جمله در مورد وضعیت روحی و جسمی آنان انجام دهد. هم‌چنین می‌توانند گروه‌هایی مانند افراد با گرایش‌های سیاسی یا شخصی خاص را امکان‌پذیر نمایند. خروجی‌های سیستم‌های هوش مصنوعی که بر داده‌های معیوب تکیه می‌کنند، می‌توانند به روش‌های مختلف به نقض حقوق بشر کمک کنند. به‌طور مثال، با علامت‌گذاری اشتباه یک فرد به‌عنوان تروریست احتمالی یا مرتکب کلاه‌برداری رفاهی، مجموعۀ داده‌های مغرضانه که منجر به تصمیمات تبعیض‌آمیز براساس سیستم‌های هوش مصنوعی می‌شود، نگران‌کننده است (Human Rights Council, 2021: 5). رمزنگاری هم‌چنان روش غالب برای حفاظت از حریم خصوصی است. هرچند که این مسأله از آن ما در مورد آن صحبت می‌کنیم، فاصله دارد. اما باید توجه داشت که رمزنگاری می‌تواند در بسیاری از مُدها برای حفاظت از حریم خصوصی در عصر داده‌های بزرگ مورد استفاده قرار گیرد (Yu, 2016: 2755).

۷. مناقشه

توسعۀ فن‌آوری های دیجیتال و اطلاعاتی در دهه‌های اخیر، به طور قابل توجهی زنده‌گی روزمرۀ ما را تحت تأثیر قرار داده است. این تحولات نوآورانه در حوزۀ فن‌آوری و اطلاعات، مزیت‌هایی را برای اجتماع داشته و باعث تغییرات ساختاری عمده‌یی در زنده‌گی روزمرۀ مردم شده و چالش‌های جدیدی را برای حفظ حق حریم خصوصی افراد به‌وجود آورده است. در دیدگاه موافقان، تکنالوژی و فن‌آوری می‌توانند بهبودهای عمده‌یی در زنده‌گی روزمرۀ ما به ارمغان بیاورند. آن‌ها معتقدند که تکنالوژی امکانات جدیدی را در دست‌رس قرار داده است، که به ما در ارتباطات، دست‌رسی به اطلاعات، نیازهای روزمره و بهبود کیفیت زنده‌گی کمک می کند. علاوه بر این، تکنالوژی می‌تواند ابزاری قدرت‌مند برای توسعۀ اقتصادی و اجتماعی باشد و به‌عنوان یک محرک اصلی برای پیش‌رفت جوامع مدرن عمل کند.

بااین‌حال، در دیدگاه مخالفان، تکنالوژی و فن‌آوری به چالش‌های جدیدی در حفظ حق حریم خصوصی افراد منجر شده است. آن‌ها معتقدند که جمع‌آوری و استفادۀ بی‌رویه از اطلاعات شخصی توسط شرکت‌ها و نهادهای دولتی، نقضی جدی به حق حریم خصوصی

ماست؛ هم‌چنین، تهدیداتی مانند هکرها، نرم افزارهای جاسوسی و حملات سایبری، حق حریم خصوصی را به‌خطر می‌اندازند و افراد را در معرض خطرات امنیتی قرار می‌دهند؛ ازسوی دیگر، تعارض بین حق حریم خصوصی و جمع‌سپاری اطلاعات در شبکه‌های اجتماعی نیز یک چالش مهم است.

باتوجه به دلایل موافقان و مخالفان در این مورد، باید گفت که تأثیر فن‌آوری در حریم خصوصی افراد مسأله‌یی پیچیده و چندجانبه است. هر دو دیدگاه دارای دلایل موجه خود هستند. بدون شک تکنالوژی زنده‌گی را برای جوامع متحول ساخته و مزیت‌های زیادی را به هم‌راه داشته است. از طرف دیگر، گه‌گاهی اثرات مضر آن نیز قابل مشاهده است. باتوجه به اهمیت روزافزون تکنالوژی و نقش آن در تمام ابعاد زنده‌گی بشری، نمی‌توان از این پدیده دوری جُست. ازسوی دیگر، اقدامات لازم «آگاهی و توان‌مندسازی افراد دربارۀ راه‌کارهای حفاظت از حریم خصوصی شخصی و اطلاعاتی، ایجاد قوانین و مقررات کارآمد در زمینۀ حفظ حریم خصوصی در فضای سایبر، قوی‌سازی رمزهای عبوری برنامه‌های اینترنتی و توجه دقیق در استفاده از سایت‌ها و اشتراک‌گذاری اطلاعات شخصی، به‌منظور حفظ حریم خصوصی در فضای سایبر امر ضروری و حتمی‌است.

۸. نتیجه‌گیری

تکنالوژی و پیش‌رفت روزافزون دیجیتال، از بزرگ‌ترین تهدیدها و چالش‌های حمایت از حریم خصوصی قلم‌داد می‌شود. با ورود به عصر تکنالوژی حفاظت از حریم خصوصی درحال تبدیل‌شدن به یک مانع اجتناب‌ناپذیر است؛ و پیش‌رفت تکنالوژی قابلیت نقض حریم خصوصی افراد را افزایش می‌دهد.

باتوجه به تحولات تکنالوژیک اخیر، چالش های بسیاری در حفظ حق حریم خصوصی افراد در عصر تکنالوژی وجود دارد. این شامل جمع‌آوری و استفادۀ نادرست از اطلاعات شخصی، تهدیدات امنیتی، و کم‌بود قوانین و سیاست‌های کامل و جامع برای محافظت از حق حریم خصوصی است. در این روند، چالش‌هاییِ مانندِ تبادل اطلاعات بین کشورها، نافرمانی شرکت‌ها در قبال قوانین حفاظت از حریم خصوصی، و نیاز به توسعۀ سیاست‌ها و قوانین جدید مطرح می‌شوند.

در عصر دیجیتال، حضور آنلاین ما بسط هویت ما است. نمایه‌های رسانه‌های اجتماعی، سایت‌های شبکه‌های حرفه یی، و ویب‌لاگ‌های شخصی نحوۀ درک دیگران از ما را شکل می دهند. بدون حفظ حریم خصوصی دیجیتال، افراد از طریق آزار و اذیت سایبری یا به

اشتراک‌گذاری غیرمجاز اطلاعات شخصی، به اعتبار خود آسیب می‌رسانند. ازسوی دیگر، پلتفرم‌های آنلاین می‌توانند محل پرورش برای آزار و اذیت، آزار و اذیت سایبری و ترور شخصیت باشند، که همه‌گی می‌توانند اعتبار یک فرد را خدشه‌دار کنند. هم‌چنین انتشار اطلاعات نادرست و اخبار جعلی حتا غیر عمد، می‌تواند به شهرت افراد آسیب برساند.

بنابراین، حریم خصوصی دیجیتال افراد را قادر می‌سازد تا کنترول بر داده‌های خود را حفظ کنند. این به این معناست که تصمیم بگیرید چه اطلاعات شخصی و با چه‌کسی به اشتراک بگذارید. بدون این کنترول، افراد ممکن است ناآگاهانه داده‌هایی را در اختیار نهادهایی قرار دهند که احتمالاً از آن برای مقاصد تجاری یا حتا مخرب سوءاستفاده کنند. به‌منظور حفاظت از حریم خصوصی داده، رمزنگاری و وضع قوانین و سیاست‌های جدی می‌تواند این روند را کاهش دهد.

۹. پیش‌نهادها و راهِ حل‌ها

الف. به‌منظور در امان‌بودن حریم خصوصی از حملات فیشینگ، اقدامات زیر می‌تواند مؤثر باشد:

۱. آموزش امنیتی: افزایش آگاهی افراد از تهدیدات امنیتی و روش‌های مقابله با حملات فیشینگ؛

۲. استفاده از فن‌آوری‌های امنیتی: نصب نرم‌افزارهای ضد ویروس، ضد بدافزار و فایروال بر روی سیستم‌ها و شبکه‌ها؛ به‌روزرسانی سیستم‌ها و نرم‌افزارها به‌صورت دوره‌یی برای افزایش مقاومت در برابر حملات؛

۳. فیلترینگ ایمیل: پیاده‌سازی فیلترهای ایمیل به‌منظور تشخیص و جلوگیری از ایمیل‌های فیشینگ، اطمینان از وجود مکانیزم‌های هُش‌دار به محض تشخیص هرگونه فعالیت مشکوک در ایمیل‌ها؛

۴. تهیه نسخهٔ پشتی‌بان: ایجاد نسخهٔ پشتی‌بان منظم از اطلاعات به‌منظور جلوگیری از دست‌رفتن اطلاعات به دنبال حملات باج‌افزار؛

۵. تعامل انسانی: آموزش کارکنان در مورد شناسایی حملات مهندسی اجتماعی و اهمیت عدم اشتراک اطلاعات حساس در سازمان‌ها و مؤسسات؛

۶. مدیریت دست‌رسی: محدودکردن دست‌رسی‌ها به اطلاعات حساس و افزایش لایه‌های احراز هویت در سازمان‌ها؛

۷. آزمون امنیتی: اجرای آزمون‌های امنیتی دوره‌یی به‌منظور شناسایی ضعف‌ها و بهبود اقدامات امنیتی؛

۸. گزارش‌گیری: تشکیل گزارش‌های دوره‌یی دربارۀ وضعیت امنیتی و تدوین راه‌کارهای بهبود اطلاع‌رسانی فوری به کاربران در مورد حملات امنیتی و تدابیر احترازی.

ب. برای حفاظت از حریم خصوصی و جلوگیری از سرقت هویت، راه حل‌های زیر پیش‌نهاد می‌گردد:

۱. آگاهی افراد: ترویج آگاهی در میان افراد دربارۀ خطرات سرقت هویت و اهمیت حفاظت از اطلاعات شخصی توسط سازمان‌های مرتبط و حامی حقوق و رسانه‌ها، کسب آموزش‌هایی دربارۀ روش‌های ایمنی در فضای آنلاین و نکاتی برای جلوگیری از سرقت هویت؛

۲. تقویت سیاست حفظ حریم خصوصی: اطمینان از وضوح و شفافیت سیاست حفظ حریم خصوصی در ویب‌سایت‌ها و سرویس‌های آنلاین، خواندن دقیق متن مربوط به سیاست حریم خصوصی برای اجازۀ ورود سیستم‌ها و سازمان‌ها به حریم خصوصی، که با رضایت و شناخت صورت گیرد؛

۳. محافظت از اطلاعات شخصی: اعمال تدابیر امنیتی مثل رمزنگاری اطلاعات حساس، محدودکردن دست‌رسی به اطلاعات شخصی و تضمین ارتقای امنیت سرورها و پای‌گاه داده‌ها؛

۴. سیاست‌گذاری قوی: اعمال سیاست‌های سخت‌گیرانه در مورد انتقال اطلاعات شخصی به صورت خودکار و بدون رضایت کاربران، اجتناب از ذخیرۀ اطلاعات شخصی بیش از حد لازم و حذف داده‌ها بلافاصله پس از انجام مراحل مورد نیاز؛

۵. توسعۀ سیاست‌های قانونی: هم‌کاری با مقامات قضایی و انجام تغییرات لازم در سیاست‌ها به منظور پیش‌گیری از نقض حریم خصوصی و پی‌گیری جرایم مرتبط.

ج. برای حفظ امنیت در استفاده از شبکه‌های وای‌فای عمومی، می‌توانید از راه حل‌های زیر استفاده کنید:

۱. استفاده از شبکه‌های مجازی خصوصی (VPN): استفاده از یک VPN به شما کمک می‌کند تا اطلاعات شخصی و ارتباطات خود را رمزگذاری کرده و از دست‌رسی هکرها جلوگیری کنید؛

۲. اطمینان از اتصال امن: هنگام استفاده از شبکه‌های وای‌فای، اطمینان حاصل کنید که اتصال شما به شبکۀ امن و رمزگذاری شده است؛

۳. عدم ارسال اطلاعات حساس: هنگام استفاده از وای‌فای عمومی، از ارسال اطلاعات حساس، مانند نام کاربری، رمزعبور و شمارۀ تلفن اجتناب نمایید؛

۴. به‌روزرسانی نرم‌افزارها: اطمینان حاصل کنید که دست‌گاه شما و نرم‌افزارهای امنیتی به‌روزرسانی شده باشند تا از آخرین امنیت‌ها بهره‌مند شوید؛

۵. قطع اتصال پس از استفاده: بعد از اتمام استفاده از شبکه وای‌فای عمومی، اتصال خود را قطع کنید تا از اطلاعات شما محافظت شود.

د. برای این‌که از اینترنت اشیا در زمینهٔ حریم خصوصی، آسیبی ایجاد نشود، راه حل‌های زیر پیشنهاد می‌گردد:

۱. استفاده از رمزهای عبور قوی: اطمینان از استفاده از رمزهای عبور قوی برای دست‌گاه‌ها و سیستم‌های اینترنت اشیا می‌تواند خطر نقض حریم خصوصی را کاهش دهد؛

۲. استفاده از حس‌گرهای امن: انتخاب حس‌گرها و دست‌گاه‌های با استانداردهای امنیتی برتر به منظور جلوگیری از نفوذ مجرمان سایبری؛

۳. مدیریت داده‌ها: پیاده‌سازی استراتیژی‌های مدیریت داده برای کاهش حجم اطلاعات و جلوگیری از انباشته‌شدن داده‌ها.

ORCID

Abdulrahman karimi https://orcid.org/0009-0004-2619-1965

سرچشمه‌ها

۱. اسکندری، مصطفی. (۱۳۸۹). «**ماهیت و اهمیت حریم خصوصی**». فصل‌نامهٔ حکومت اسلامی. سال ۱۵. شمارهٔ ۴. https://www.noormags.ir/view/fa/articlepage/947537.

۲. امامی، سید حسن. (۱۳۸۷). **شرح قانون مدنی**. چ۲۸. ج۱. تهران: انتشارات اسلامیه.

۳. انصاری، باقر. (۱۳۸۶). **حقوق حریم خصوصی**. قم: گل‌ها.

انصاری، باقر. (۱۳۹۳). «**حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران**». دانش‌گاه تهران: مجلهٔ دانش‌کدهٔ حقوق و علوم سیاسی دانشگاه تهران. شمارهٔ ۶۶. https://ensani.ir/fa/article/16761.

۴. بیستونی، صفورا؛ مقدادی، محمدمهدی. (۱۴۰۱). «**بررسی تطبیقی گسترهٔ حریم خصوصی کودک در اسلام و کنوانسیون حقوق کودک**». نشریهٔ علمی حقوق تطبیقی معاصر. سال ۱۳. شمارهٔ ۲۸. https://ensani.ir/fa/article/536868.

۵. جعفری لنگرودی، محمدجعفر. (۱۳۸۷). **ترمینولوژی حقوق**. چ۱۰. تهران: انتشارات گنج دانش.

۶. خرم‌دل، مصطفی. (۱۳۸۸). **تفسیر نور**. چ۷. تهران: نشر احسان.

۷. خویی، سید ابوالقاسم. (۱۴۱۰ق). **منهاج الصالحین**. چ۲۸. ج۲. قم: مدینهٔ العلم.

۸. رئوفی، علی‌اصغر و هم‌کاران. (۱۳۹۹) «**اصول حاکم بر لایحهٔ حریم خصوصی**». فصل‌نامهٔ مبانی فقهی حقوق اسلامی. سال ۱۳، شمارهٔ ۲۵. https://journals.srbiau.ac.ir/article_16350.html.

۹. عبداله‌زاده، انس؛ حاجی پورکندرود، علی. (۱۴۰۱) «**تحلیل چالش‌های دولت الکترونیک با حریم خصوصی اطلاعاتی شهروندان**». فصل‌نامهٔ حقوق اداری. ۹(۳۱). https://qjal.smtc.ac.ir/article-1-1030-fa.pdf.

۱۰. علامه حلی، حسن بن یوسف بن مطهر اسدی. (۱۴۱۴ق). **تذکره الفقهاء**. قم: مؤسسه آل البیت علیهم الاسلام.

۱۱. علی حسینی، همایون علی و هم‌کاران. (۱۳۹۹). «**امنیت محتوای داده‌ها در حریم خصوصی و مطالعه تطبیقی آن**». فصل‌نامۀ علمی – پژوهشی جامعه‌شناسی سیاسی ایران. ۳(۲). پیاپی ۱۰. https://www.noormags.ir/view/fa/articlepage/120025/1079.

۱۲. فتحی، یونس؛ شاه‌مرادی، خیراله. (۱۳۹۶) «**گسترۀ قلم‌رو حریم خصوصی در فضای مجازی**». مجلۀ حقوقی دادگستر. ۸۱ (۹۹). https://www.jlj.ir/article_29234.

۱۳. قهفرخی، شهباز؛ مسعودیان، مصطفی. (۱۳۹۱). «**حمایت از حریم خصوصی از منظر آیات و روایات**». دوفصل‌نامۀ تخصصی پژوهش‌های میان‌رشته‌یی قرآن کریم. ۳ (۲). https://ensani.ir/fa/article/download/522480.

۱۴. کاتوزیان، ناصر. (۱۳۹۴). **قانون مدنی در نظم حقوقی کنونی**. چ۴۶. تهران: انتشارات میزان.

۱۵. مازندرانی، محمد صالح ابن احمد بن شمس سوری. (۱۳۸۲). **شرح الکافی**. چ۲. تهران: انتشارات اسلامی.

۱۶. مصطفوی اردبیلی، سید محمدمهدی؛ تقی انصاری، مصطفی؛ رحمتی‌فر، سمانه. (۱۴۰۲). «**تأثیر هوش مصنوعی بر نظام حقوق بشر بین‌الملل**». دوفصل‌نامۀ حقوق فناوری‌های نوین. ۴(۸).

۱۷. معین، محمد. (۱۳۶۳). **فرهنگ فارسی معین**. چ۲. چ۹. تهران: انتشارات امیرکبیر.

۱۸. موسوی بجنوردی، سید محمد؛ نسترن‌پور. (۱۳۹۷). «**بررسی فقهی و حقوقی حریم خصوصی**». مجلۀ نامۀ الهیات. ۱۱(۴۲). https://sanad.iau.ir/journal/jt/Article/663969?jid=663969.

19. Alessandro. A, Laura. B & George. L. (2015) Privacy and Human Behavior in the Age of Information, Science, Volume 347, No 6221, PP 509-514.
https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.

20. Radi P. Romansky & Irina S. Noninska. (2020) Challenges of the digital age for privacy and personal data protection, Mathematical Biosciences and Engineering(MBE), volume17(5) PP 5288-5303.
https://www.aimspress.com/article/id/5544

21. Yu. S (2016) Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data, IEEE Access, Volume 4, PP 2751-2763.
https://feihu.eng.ua.edu/NSF_BD_lec15.pdf

22. Rashidat Taiwo. A (2023) Personal Protection of Privacy in the Information Age, Library Philosophy and Practice (e-journal), pp 1-15.
https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=15127&context=libphilprac

23. Griffin. K, Whitehead. R, Balsmeier. P & Packer. J (2002) Privacy in The Age of Technology, International Business & Economics Research Journal, Volume 1, Number 4, pp 29-38.
https://www.clutejournals.com/index.php/IBER/article/view/3911

24. Brandqvist. J & Lieberth Nilsson. J (2023) Phishing Detection Challenges for Private and Organizational Users: A Comparative Study Bachelor Degree Project in Informatics, university of Skovde.

25. Lotfy. A, Zaki. A, Hafeez, T & Mahmoud. T, (2021) Privacy Issues of Public Wi-Fi Networks, In book: Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), pp.656-665.
https://www.researchgate.net/publication/351947401
26. Schermer. B, (2011) The limits of privacy in automated profiling and data mining, ELEVIER, volume 27, Issue 1, pp 45-52.
https://www.sciencedirect.com/science/article/abs/pii/S0267364910001767
27. Human Rights Council, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Forty-eighth session, 13 September–1 October 2021, Agenda items 2 and 3

References

1. Ansari, Bagher. (2007). Privacy Rights, 1st Edition, Qom, Golha Publishing. (Persian)
2. Emami, Seyyed Hassan. (2008). Explanation of Civil Law, 28th Edition, Tehran, Islamic Publications, Volume 1. (Persian)
3. Jafari Langroudi, Mohammad Jafar. (2008). Legal Terminology, 10th Edition, Tehran: Ganj Danesh Publications.
4. Khorddel, Mostafa. (2009). Interpretation of Noor, 7th Edition, Tehran, Ehsan Publishing. (Persian)
5. Khoyi, Seyyed Abolghasem. (1931). Manhaj al-Salihin, 28th Edition, Qom, Madinat al-Ilm, Volume 2. (Persian)
6. Allameh Hilli, Hasan ibn Yusuf ibn Mutahhar Asadi. (1435). Tazkirat al-Fuqaha, Qom, Al al-Bayt Institute. (Persian)
7. Katuzian, Naser. (2015). Civil Law in the Current Legal Order, 46th Edition, Tehran: Mizan Publications. (Persian)
8. Mazandarani, Mohammad Saleh ibn Ahmad ibn Shamsouri. (2003). Sharh al-Kafi, Vol. 6, Tehran, Islamic Publications. (Persian)
9. Mo'in, Mohammad. (1984). Mo'in Persian Dictionary, 2nd Edition, Tehran, Amir Kabir Publications, Vol. 9. (Persian)
10. Ansari, Bagher. (2014). "Privacy and Its Protection in Comparative Islamic and Iranian Law," University of Tehran, Faculty of Law and Political Science Journal, No. 66. (Persian)
11. Eskandari, Mostafa. (2010). "The Nature and Importance of Privacy," Islamic Government Quarterly, 15th Year, No. 4. (Persian)
12. Biston, Safura, Moghaddadi, Mohammad Mehdi. (2022). "A Comparative Study of the Scope of Children's Privacy in Islam and the Convention on the Rights of the Child," Contemporary Comparative Law Journal, 13th Year, No. 28. (Persian)
13. Raufi, Ali Asghar, Jamshidi Rad, Mohammad Sadegh, and Pour Bafarani, Alireza. (2020). "Principles Governing the Privacy Bill," Islamic Legal Foundations Quarterly, 13th Year, No. 25. (Persian)
14. Ali Hosseini, Homayoun Ali, Karami, Hamidreza, and Ahmadi Far, Rasoul. (2020). "Data Content Security in Privacy and Its Comparative Study," Iranian Journal of Sociopolitical Sociology, 3rd Year, No. 2, Issue 10. (Persian)
15. Abdolhazadeh, Enas, and Hajipour Kandroud, Ali. (2022). "Analysis of Challenges of E-Government with Citizens' Information Privacy," Administrative Law Journal, 9th Year, No. 31. (Persian)
16. Fathi, Younes, and Shahmoradi, Khairallah. (2017). "The Scope of Privacy in the Virtual Space," Dadgostar Legal Journal, 81st Year, No. 99. (Persian)

17. Ghafori, Shahbaz, and Masoudian, Mostafa. (2012). "Protection of Privacy from the Perspective of Verses and Narrations," Interdisciplinary Quranic Research Biannual, 3rd Year, No. 2. (Persian)
18. Mousavi Bajnourdi, Seyyed Mohammad, and Nastaranpour. (2018). "Jurisprudential and Legal Examination of Privacy," Theological Journal, 11th Year, No. 42. (Persian)
19. Mostafavi Ardabili, Seyyed Mohammad Mehdi, Taghi Ansari, Mostafa, and Rahmati Far, Samaneh. (2023). "The Impact of Artificial Intelligence on the International Human Rights System," Journal of New Legal Technologies, Volume 4, No. 8. (Persian)
20. Alessandro. A, Laura. B & George. L. (2015) Privacy and Human Behavior in the Age of Information, Science, Volume 347, No 6221, PP 509-514.
https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.
21. Radi P. Romansky & Irina S. Noninska. (2020) Challenges of the digital age for privacy and personal data protection, Mathematical Biosciences and Engineering(MBE), volume17(5) PP 5288-5303. https://www.aimspress.com/article/id/5544
22. Yu. S (2016) Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data, IEEE Access, Volume 4, PP 2751-2763.
https://feihu.eng.ua.edu/NSF_BD_lec15.pdf
23. Rashidat Taiwo. A (2023) Personal Protection of Privacy in the Information Age, Library Philosophy and Practice (e-journal), pp 1-15.
https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=15127&context=libphilprac
24. Griffin. K, Whitehead. R, Balsmeier. P & Packer. J (2002) Privacy in The Age of Technology, International Business & Economics Research Journal, Volume 1, Number 4, pp 29-38. https://www.clutejournals.com/index.php/IBER/article/view/3911
25. Brandqvist. J & Lieberth Nilsson. J (2023) Phishing Detection Challenges for Private and Organizational Users: A Comparative Study Bachelor Degree Project in Informatics, university of Skovde.
26. Lotfy. A, Zaki. A, Hafeez, T & Mahmoud. T, (2021) Privacy Issues of Public Wi-Fi Networks, In book: Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021), pp.656-665.
https://www.researchgate.net/publication/351947401
27. Schermer. B, (2011) The limits of privacy in automated profiling and data mining, ELEVIER, volume 27, Issue 1, pp 45-52.
https://www.sciencedirect.com/science/article/abs/pii/S0267364910001767
28. Human Rights Council, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Forty-eighth session, 13 September–1 October 2021, Agenda items 2 and 3